STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy No. DOC 1.7.7	Subject: **COMPUTER SECURITY**	
Chapter 1: ADMINISTRATION AND MANAGEMENT		Page 1 of 3 and Attachment
Section 7: Information Systems		Effective Date: Dec. 1, 1996
Signature: /s/ Mike Ferriter, Director		Revised: 04/26/07 Reviewed: 12/15/08

I. POLICY

The Department of Corrections administers computer security to prevent the intentional or unintentional modification, destruction, disclosure, or misuse of data and information technology resources, and to remain in compliance with state laws and policy.

II. APPLICABILITY

All divisions, facilities, or programs under Department jurisdiction or contract.

III. DEFINITIONS

Data and Information Technology Resources – The State mainframe computer; the State's and the Department's mid-range computers and file servers; the Internet and intranet; Local and Wide Area Networks (LANs & WANs) and associated equipment; microcomputer hardware and software, printers and other peripherals; facility resources related to computing, electronically stored data, and other related resources.

Password – An alphanumeric combination of characters unique to individual users that allows access to a specific computer, network or computer system.

User ID – Used generically to refer to CI number, login ID, ACF2 ID, user account, or any other term used to describe a user's unique identifier which is used to grant rights and privileges on a computer, computer system or network. User IDs are never reused.

IV. DEPARTMENT DIRECTIVES

A. General

1. The Department has delegated its statutory authority for the security of data and information technology resources to the Information and Business Technology Bureau of the Health, Planning and Information Services Division. The bureau will appoint a security officer(s) to handle the day-to-day activities related to providing staff with access to the systems and data that they need to perform their jobs.

2. Department data, in general, belongs to the Department's various programs. The Information and Business Technology Bureau (IBTB) functions as the "caretaker" of data for the programs by granting and restricting access to that data on behalf of the owners of each set of data. Therefore, each facility, program or division will appoint a security coordinator to work with IBTB on security matters. The security coordinators will

receive requests from local staff for new or changed access to systems and data and, when approved, forward them to the IBTB security officer through the IT Help Desk for implementation. The program to which the data "belongs" must approve the requests from one program for access to another program's systems or data.

3. The security officer may develop and implement additional procedures deemed to be in the best interests of protecting the integrity of, and access to, Department data and information technology resources. In all cases, the security officer and/or local security coordinators will be conservative regarding security issues.

4. The Information and Business Technology Bureau grants data access on a “most restrictive” or “least rights” basis; users are granted the lowest level of access possible to accomplish their job functions.

5. Local security coordinators will notify the security officer, through the IT Help Desk, whenever an employee changes positions within the Department, and request appropriate changes to the employee’s access rights. Security coordinators will also notify the IT Help Desk when staff terminate so that their access to systems and data can be terminated.

B. User ID and Passwords

1. Each employee allowed access to any Department information system will be assigned a User ID and password for these systems. Also, applications that run on these systems may require a separate User ID and password. Prior to any staff member being issued a User ID and password, which are required to access the network, they must read this policy and Department IT *Policies 1.7.3, 1.7.6, and 1.7.9* and provide documentation of such by filling out and signing the attached IT Consent Form and returning it to the IT Help Desk.

2. The User IDs and passwords grant specific rights to users that vary from user to user depending upon the requirement of their job. For example, Employee “A” may have a User ID that allows access to all parts of the Adult Criminal Information System (ACIS) while Employee “B's” User ID grants access to only certain parts of ACIS.

3. Each employee must protect the confidentiality of his/her User ID and password. Employees may not share nor in any way divulge User IDs and passwords to others, nor write them down and leave them where others may find them.

4. Employees will not stay signed onto systems when they are going to be absent from the computer or terminal for fifteen minutes or longer and, unless otherwise directed, must sign off of systems when they leave the work area at night.

5. If employees violate this policy, their computer security rights will be immediately terminated. Supervisors may not reinstate individual computer rights before assuring the security officer that steps have been taken to prevent further violations.

6. The IBTB may grant emergency access to an absent employee's data and/or email account if approved by the appropriate supervisor from the program owning the data.

Such requests will be made in writing, have a limited time frame, and be evaluated on a case-by-case basis by the security officer.

V. CLOSING

Questions concerning this policy should be directed to the CIO or the IT Policy and Strategic Planning Officer.

VI. REFERENCES

A. *2-15-112, MCA (2007) Duties and Powers of Department Heads; 2-15-114, MCA (2007) Security Responsibilities of Departments for Data; 2-17-534, MCA (2007) Security Responsibilities of Department*

B. *1-0250.00 Montana Operations Manual*

C. *ENT-SEC-063, ENT-SEC-072; Enterprise IT Policy*

D. *DOC Policies 1.7.3, Data Quality; 1.7.6, Unlawful Use of Computers; 1.7.9, Acceptable Use of IT Resources*

VII. ATTACHMENT

IT Consent Form